WHAT IS CLAIMED IS:

1. A communication system having a server for providing a Web E-mail service to a client, wherein said server comprises:

management means for managing a key for decrypting an encrypted E-mail;

decrypting means for decrypting said encrypted E-mail using said managed key; and

transmission control means for controlling said decrypted E-mail thereby to transmit said decrypted E-mail to said client through a Web.

2. The communication system according to claim 1, wherein said server further comprises:

authentication means for executing authentication of the use allowance of said key to said client, and

said decrypting means decrypts said encrypted E-mail in the case where the use allowance is authenticated by said authentication means.

3. The communication system according to claim 2, wherein said authentication means provides said client with a window data to authenticate the use allowance of said key.

4. The communication system according to claim 2, wherein said authentication means authenticates the use

allowance using a passphrase inputted from said client.

5. The communication system according to claim 2, wherein said authentication means authenticates the use allowance using a biometrics information inputted from said client.

6. The communication system according to claim 1, wherein said server further comprises encryption communication means for establishing and communicating a Web encryption communication when communicating with said client through the Web.

7. The communication system according to claim 2, wherein said server further comprises the encryption communication means for establishing and communicating the Web encryption communication when communicating with said client through the Web, and transmission means for transmitting the use allowance by said authentication means and the E-mail decrypted by said decrypting means to said client after the Web encryption communication is established by said encryption communication means.

8. The communication system according to claim 7, wherein said authentication means authenticates the use allowance of said key in units of a session of an

encryption communication continuously established between said client and a server.

9. The communication system according to claim 8, wherein said authentication means stops said authenticated use allowance, in the case where at least either the case where said encryption communication is ended with an error or the case where said encryption communication has passed a fixed time is satisfied.

10. The communication system according to claim 1, wherein said server further comprises signature means for executing a digital signature to an E-mail required for the digital signature by said client.

11. The communication system according to claim 1, wherein said server further comprises:

management means for managing whether said key is under multiple use, and

said management means comprises stop means for stopping the use allowance of said session under multiple use in the case where said session is judged to be under multiple use.

12. The communication system according to claim 1, wherein the key for decrypting said encrypted E-mail is a secret key in a code of a public key cryptosystem.

13. The communication system comprising:

management means for managing a key for decrypting an encrypted E-mail;

decrypting means for decrypting said encrypted E-mail using said managed key; and

a client receiving a Web E-mail service from a server including transmission control means for controlling said decrypted E-mail so as to transmit to said client through the Web,

wherein said client comprises the use allowance means for executing use allowance of the key for decrypting said encrypted E-mail to said server, and receiving means for receiving the E-mail decrypted by said server through the Web.

14. A method for controlling a communication system including a server for providing the client with the Web E-mail service, comprising:

a management step of managing a key for decrypting an encrypted E-mail;

a decrypting step of decrypting said encrypted E-mail using said managed key; and

a transmission control step of controlling said decrypted E-mail to transmit to said client, in the server.

15. A method for controlling the communication

system according to claim 14, further comprises an authentication step of authenticating use allowance of said key to said client in the server, wherein said encrypted E-mail is decrypted in said decrypting step in the case where the use allowance is authenticated in said authentication step.

16. A method for controlling the communication system according to claim 15, wherein, in said authentication step, a window data for authenticating the use allowance of said key is supplied to said client for authentication.

17. A method for controlling the communication system according to claim 15, wherein, in said authentication step, the use allowance is authenticated using a passphrase inputted from said client.

18. A method for controlling the communication system according to claim 15, wherein, in said authentication step, the use allowance is authenticated using biometrics information inputted from said client.

19. A method for controlling the communication system according to claim 14, wherein, in said server, the method further comprises an encryption communication step of establishing and communicating

the Web encryption communication when communicating with said client through the Web.

20. A method for controlling the communication system according to claim 15, in said server, further comprising the encryption communication step of establishing and communicating the Web encryption communication when communicating with said client through the Web, and a transmission control step of transmitting use allowance in said authentication step and the E-mail decrypted by said decrypting step to said client after the Web encryption communication is established in said encryption communication step.

21. A method for controlling the communication system according to claim 20, wherein, in said authentication step, the use allowance of said key is authenticated in units of a session of an encryption communication continuously established between said client and a server.

22. A method for controlling the communication system according to claim 21, wherein, in said authentication step, said authenticated use allowance is stopped in the case when at least either the case where said encryption communication is ended with an error or the case where said encryption communication

has passed a fixed time is satisfied.

23. A method for controlling the communication system according to claim 14, further comprising a signature step of executing the digital signature to the E-mail required for the digital signature from said client in said server.

24. A method for controlling the communication system according to claim 14, further comprising a step of executing a management step of managing whether said key is under multiple use in the server, said management step including a stop step of stopping the use allowance of the session under multiple use in the case where the session is judged to be under multiple use.

25. A method for controlling the communication system according to claim 14, wherein the key for decrypting said encrypted E-mail is a secret key in an encryption of a public key cryptosystem.

26. A method for controlling a communication system including a client receiving a Web E-mail service from a server, comprising a step of executing a management step of managing a key for decrypting an encrypted E-mail, a decrypting step of decrypting said

encrypted E-mail using said managed key and a transmission control step of controlling said decrypted E-mail so as to transmit to said client in the server, and comprising a step of executing a use allowance step of executing the use allowance of the key of decrypting said encrypted E-mail, and a receiving step of receiving the E-mail decrypted by said server in the client.

27. A computer executable control program of a communication system including a server for providing a Web E-mail service to a client, said program comprising a management step of managing a key for decrypting an encrypted E-mail, a decrypting step of decrypting said encrypted E-mail using said managed key, and a transmission control step of controlling said decrypted E-mail so as to transmit to said client.

28. A control program of a communication system including a client receiving a Web E-mail service through a Web from a server, comprising a step of executing a management step of managing a key for decrypting an encrypted E-mail, a decrypting step of decrypting said encrypted E-mail using said managed key, and a transmission step of controlling said decrypted E-mail so as to transmit to said client in the server, and said client comprising a step of

executing a use allowance step of executing the use allowance of the key for decrypting said encrypted E-mail to said server, and a receiving step of receiving the E-mail decrypted by said server in the client.

29. A storage medium storing a computer executable control program of a communication system including a server of providing a Web E-mail service to a client, the program comprising a step of executing a management step of managing a key for decrypting said encrypted E-mail using said managed key, and a transmission control step of controlling said decrypted E-mail so as to transmit to said client in a server.

30. A storage medium storing a control program of a communication system including a client receiving a Web E-mail service through a Web from a server, wherein the program comprises a step of executing a management step of managing a key for decrypting an encrypted E-mail, a decrypting step of decrypting said encrypted E-mail using said managed key in the server, and a transmission control step of controlling said decrypted E-mail so as to transmit to said client, and wherein the program comprises a step of executing a use allowance step of executing the use allowance of a key for decrypting said encrypted E-mail to said server and a receiving step of receiving the E-mail decrypted by said server.